GIDEON AntiVirus BLOC system

ギデオン ブロックシステム
製品紹介

会社紹介

社名	株式会社ギデオン
設立	1990年1月
本社所在地	横浜市港北区
主要製品	ギデオン アンチウイルス
	ギデオン アンチスパムPlus
	ギデオン ゲートセキュリティ
	ギデオン BLOC system

スパム対策の重要性

一方的に大量配信される不用なメール。商業宣伝・広告、デマやいたずらのチェーンメールなど種類もさまざま、発信元を偽り無差別に配信し、中には不正なメールサーバ利用もあります。その被害はウイルスの次に多く、スパイウェアや個人情報の流出、ワンクリック詐欺など今や社会問題とされています。

業務効率の悪化　→　スパム選別の無駄な時間
インフラへの負荷　→　メールサーバ処理能力低下、ネットワーク負荷
セキュリティへの脅威　→　ウイルス、スパイウェア、フィッシング詐欺

一般的なスパム対策方法(課題)

・クライアントメーラーで振り分け管理する。

→　迷惑メール誘導URLによるワンクリック詐欺などの対応

・アプライアンス機器導入

→　自社メールサーバを持っていないと導入できない。
(多くがSMTPしかサポートしていない)

→　リモートにあるメールサーバからメールを取得し、
localhostのSMTPサーバを通じて自分宛に転送する
フェッチメール(クライアントメーラー設定変更が必要)

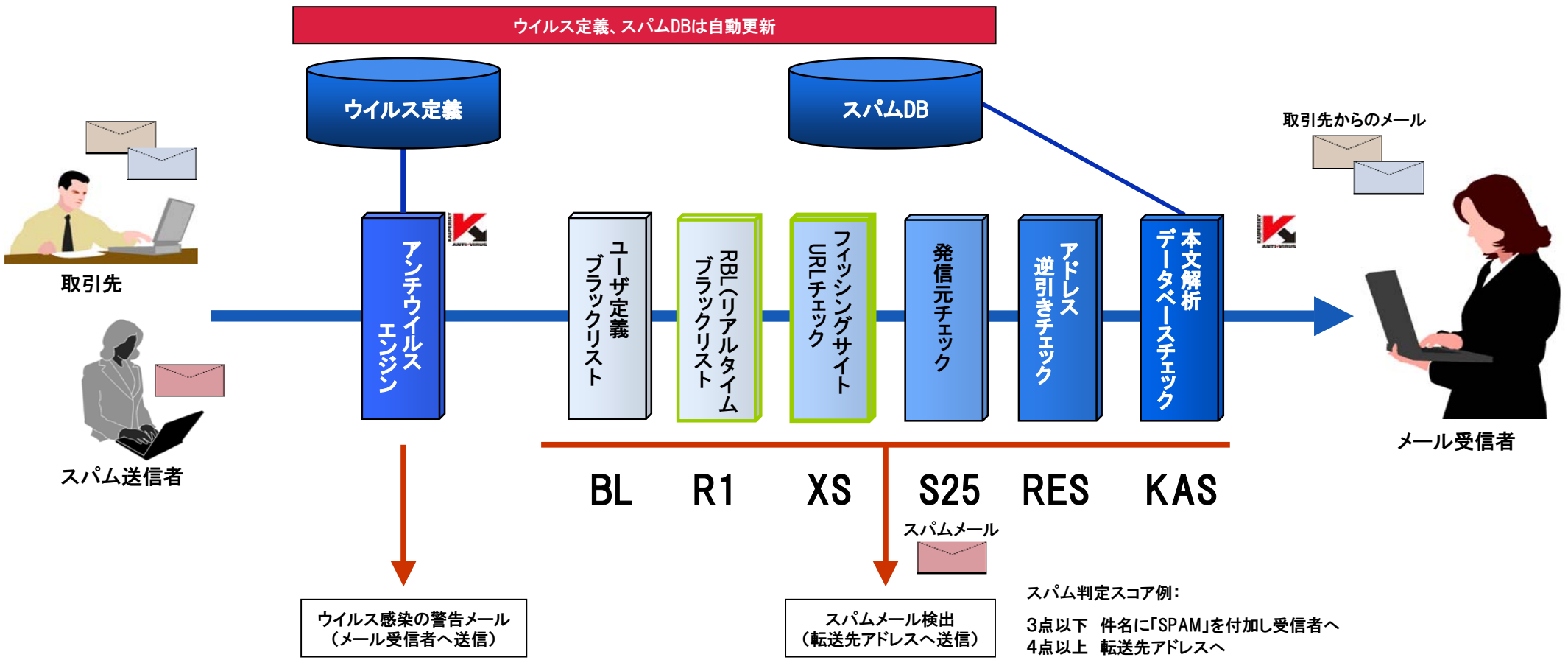
・ホスティングの迷惑メールサービスを利用

→　サービスに制限がある。
誤検知・削除されてしまった場合のサポート

BLOC system PortControl Plusの特徴

- POP3・SMTPに対応したスパム/ウイルス対策アプライアンス機器
  （ホスティングのメールサーバ利用でも導入可能）
- 透過ブリッジ方式で既存の環境に導入可能
  （周辺ネットワーク機器の設定変更が最小限に抑えられる）
- POP3によるスパムメールの転送機能・削除機能
- 50ユーザから1,000ユーザまで対応
- スパムDBは3時間ごとに自動更新

ウイルス検知・スパムフィルタリング



GIDEON　スパムフィルタについて

BL(スコア:4)　お客様にてブラックリストとして、送信元IP(host)または
envelopeのFromメールアドレス・Toメールアドレスを
登録することが可能です。

R1(スコア:3)　4箇所のRBLを参照し、ブラックリストに登録されていないか
確認をします。

bl.gideon.co.jp　sbl-xbl.spamhaus.org　bl.spamcop.net　all.rbl.jp

XS(スコア:3)　URLフィルタリング。本文中の誘導先URL参照し、
ブラックリストに登録されていないか確認をします。
URLはエンコードされたものはデコードしチェックを行います。

bl.gideon.co.jp　url.rbl.jp　dyndns.rbl.jp　multi.surbl.org

S25(スコア:1) メールヘッダのReceivedに記述された命名規則がスパムで
よく用いられる形式かどうか(形式チェック)
(逆引きホストの命名則、PPP 等の命名則などADSLを
使った個人配信の可能性など)

RES(スコア:1) 送信元IPアドレスからドメインの逆引きができるか。

KAS(スコア:3) メッセージ解析、750万件のスパム定義データベース。
メール形式の不正チェック、ロジカルな構文チェック。
※スパム判定は6項目の判定方法の合計値で判定を行っております。
(スパムの誤検知率を下げるため、複数基準の適用を標準。)

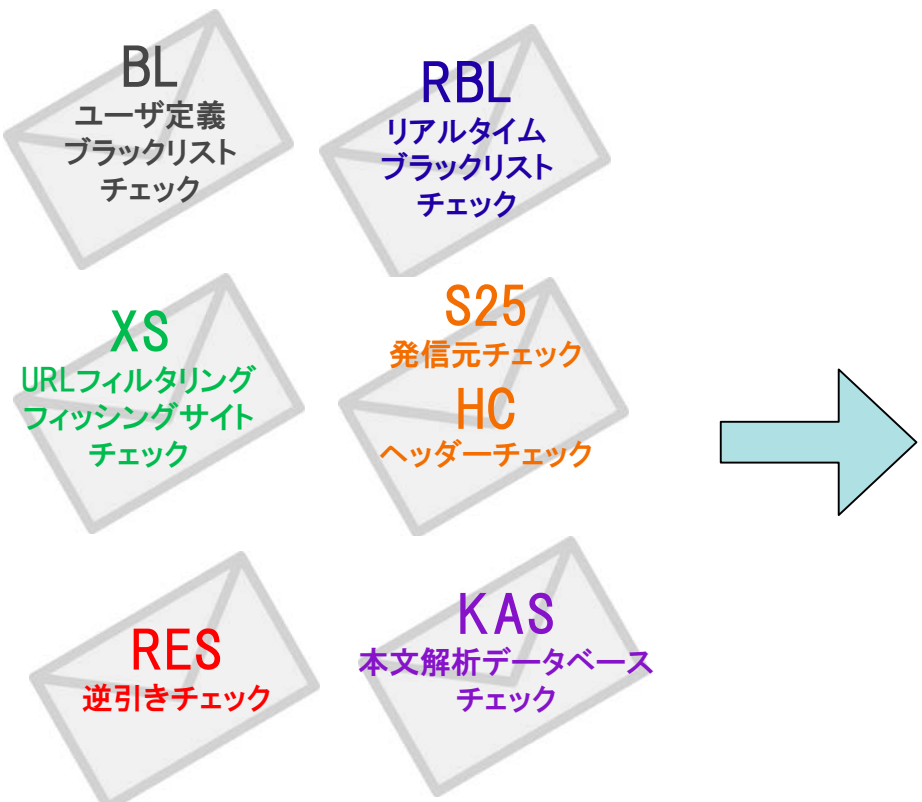
bl.gideon.co.jp について

・R1・XSは、メール1通受信するごとに外部参照先に対し、問い合わせを行い
ブラックリスト登録されていないか確認を行っております。
その際、当社スパムDBサイト「bl.gideon.co.jp」へもアクセスがあります。

現在、ご利用いただいている企業ユーザ約100万アカイントが
メールを受信するリアルタイムで 「bl.gideon.co.jp」 に
「 送信元IP 」「 URL 」を参照します。
このアクセスログを自動解析・自動登録をリアルタイムで行い、
ご利用いただいてるお客様へいち早く提供することにより、
スパム検知率アップしております。

他社とのスパムフィルタの違い

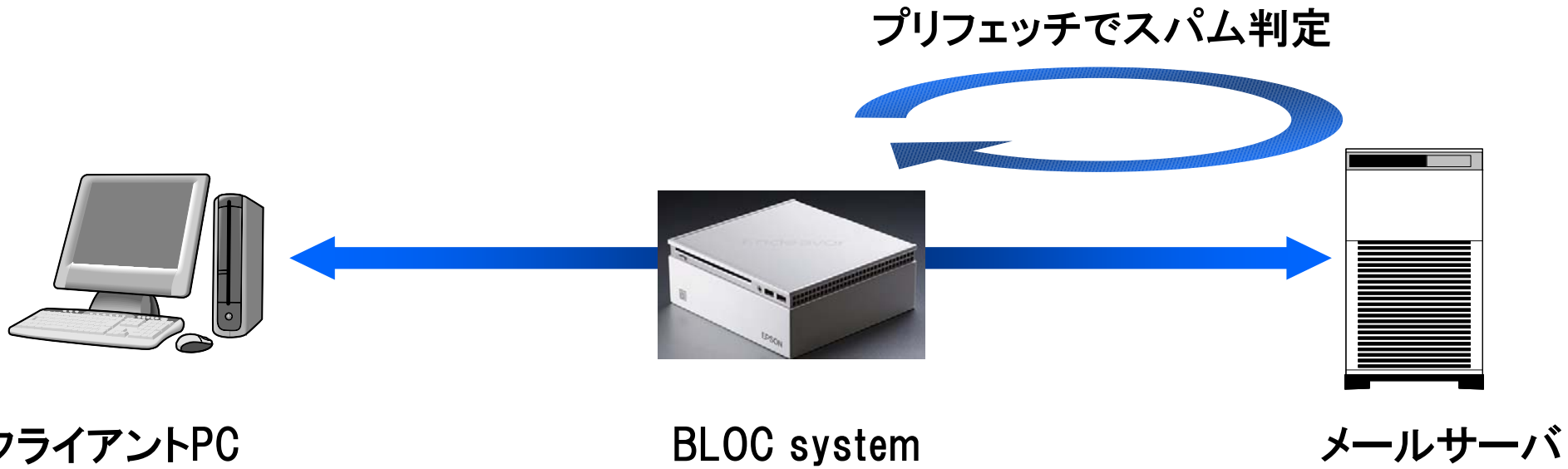
多くのアンチスパムソフトは、主にベイジアン理論（用語に依存した条件確率）を用いていますが、ギデオンでは<u>スパムデータベースとメールを照合する手法</u>で検知率アップを実現。



メールヘッダと本文の例

```
Received: from ppp-hoge.net (ppp-hoge.net [209.102.244.192])
by xxx.domain.co.jp (Postfix) with SMTP id 9B84D5A4002
for <xxx@domain.co.jp>; Wed, 25 Oct 2006 13:28:48 +0900 (JST)
From: "中塚賀織" <kaori@private.udn.ne.jp>
Reply-To: "中塚賀織" <kaori@private.udn.ne.jp>
Reply-To: <taiowghget@private.udn.ne.jp>
To: info@domain.co.jp
Subject: メンチじゃないミンチカツ
Date: Tue, 24 Oct 2006 21:09:10 -0800
X-Info:info@domain.co.jp
X-Message-Info: sukjlroivcndu7jsg
MIME-Version: 1.0
Content-Type: text/plain
List-Id: 8
Message-Id: <AUNYTYRK$UIKYTR@domain.co.jp>


中塚賀織
2006年10月24日
info@domain.co.jp
メンチじゃないミンチカツ

http://92181.ss.com:112/ol-ot-f/
出会い系サイトを運営している奈津美と申します。
今年は女性会員獲得にレディコミ投稿や駅前でのティッシュ配布に2億を投資した結果男性会員との比率が8:2になってしまい、女性からの苦情が出てしまって困っています。そのためあなたを永久的に完全無料でお使いいただ ける特別会員になっていただきたいと思っております。ニックネームの最後に「★」を付けていだければこちらのほうで特別会員に設定させていただきま
http://92181.ss.com:112/ol-ot-f/
ゆっくりと高齢のお金もちの女性を見つけてリッチな生活を送ってみてください。

自信がない方はnatumi3211@enet.com.cn

----321126239600726----------
```

BLOC system のプリフェッチ機能



・クライアントPCでのメール受信と同じ動作をBLOCが行う仕組み。

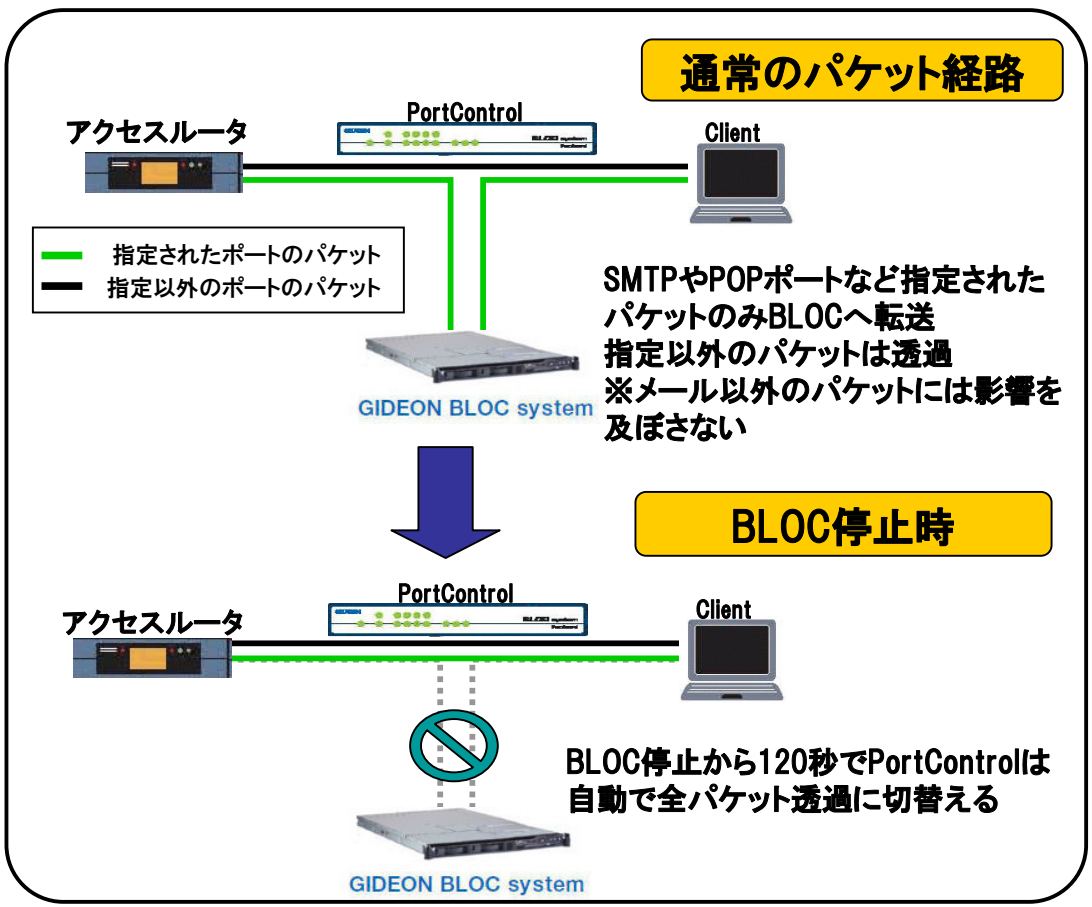
・BLOCがサーバのメールボックスメールを巡回しながらチェック。

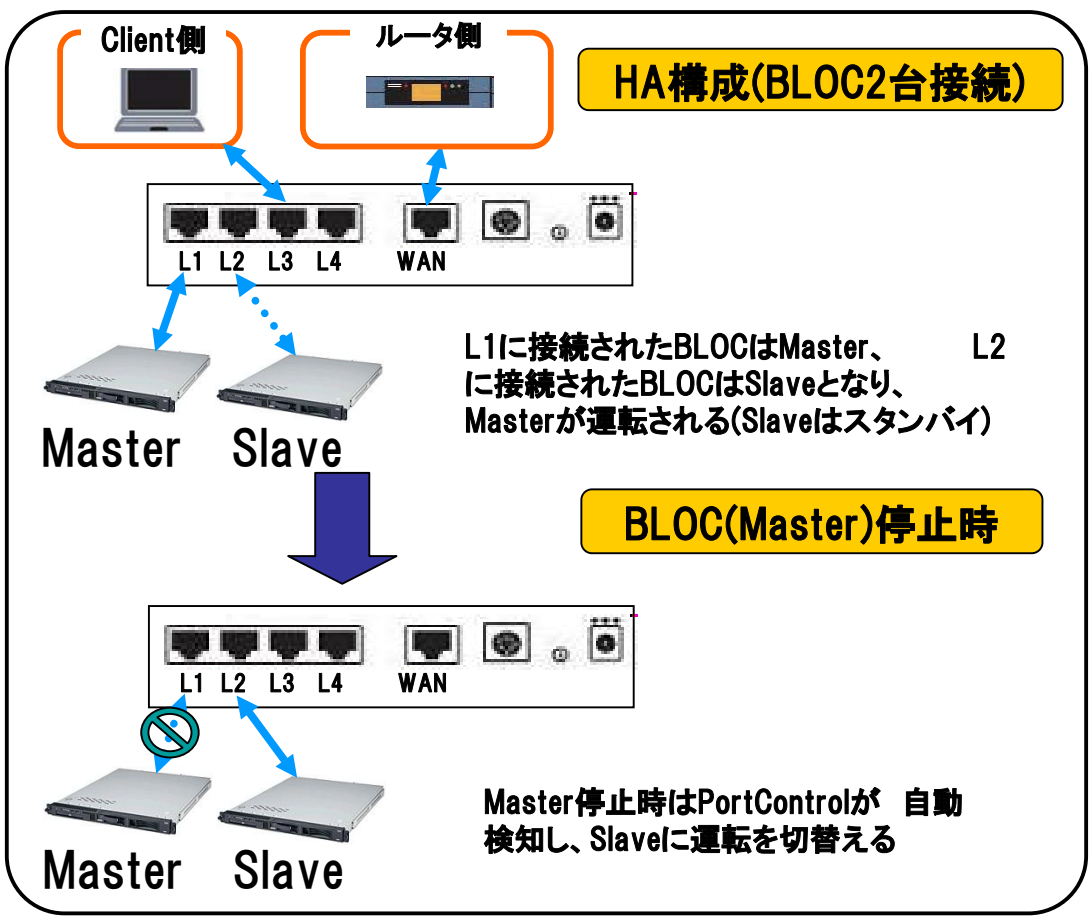
・1プロセス　：　10メールボックス　10通

・スコアに達した場合は、メール転送後・メールボックス内
スパムメールを削除します。

機能説明-PortControl

- 通過するパケットを指定し、BLOCへ転送(指定パケット以外にはネットワークに影響を与えない)
- BLOCへ向けてキープアライブ通信を実施
  - BLOCが停止すると、全パケット透過に自動切換
  - BLOCを2台接続したHA構成をとった場合、MasterのBLOCが停止すると、SlaveのBLOCに自動切換





・自社にメールサーバがない場合でもスパムの除去・転送が可能

・24時間稼働なので、処理負荷の軽減、クライアント処理の軽減

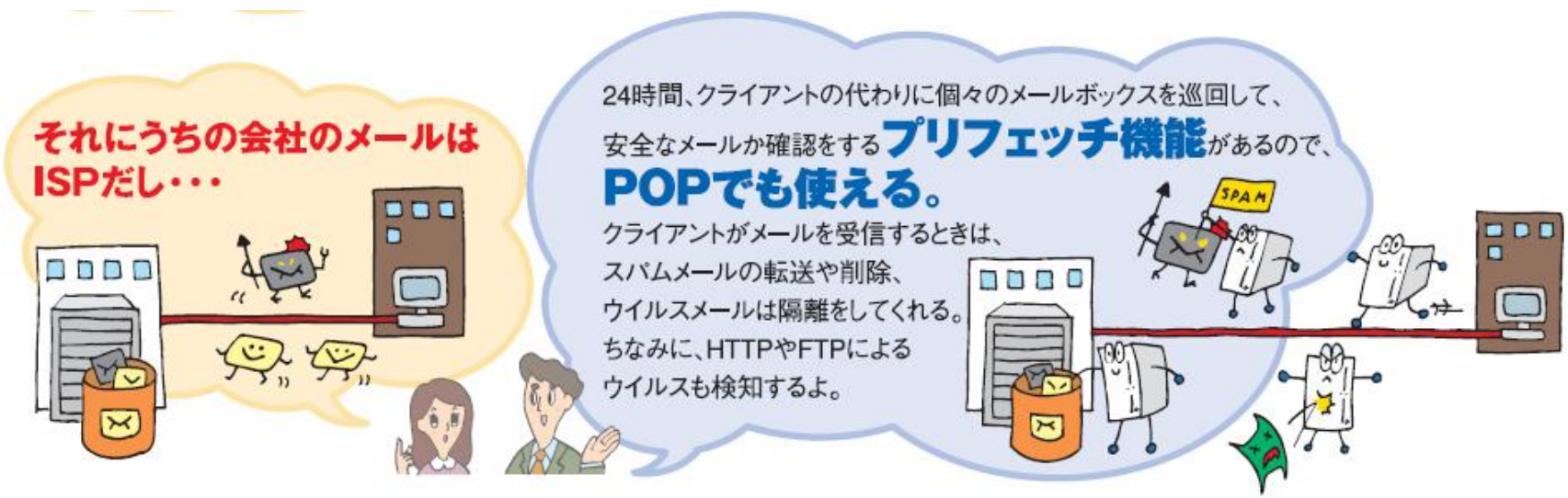
・運用形態に沿った設定が可能

　チェックリスト/ホワイトリスト/ブラックリストのユーザ毎設定、

　プリフェッチ動作時間設定　etc

・BLOCにはデータを保持しないので、BLOC障害時でもメールデータを

　紛失しません。



スパム判定実測結果

2008年1月ユーザ様サイトで1週間スパムメールを受信。

判定結果内訳

98%	スパムとして検知(総合スコア4点以上)
1.99%	スパムの可能性ありとして検知(総合スコア3点)
0.01%	スパムとして検知せずスルー
0%	誤検知

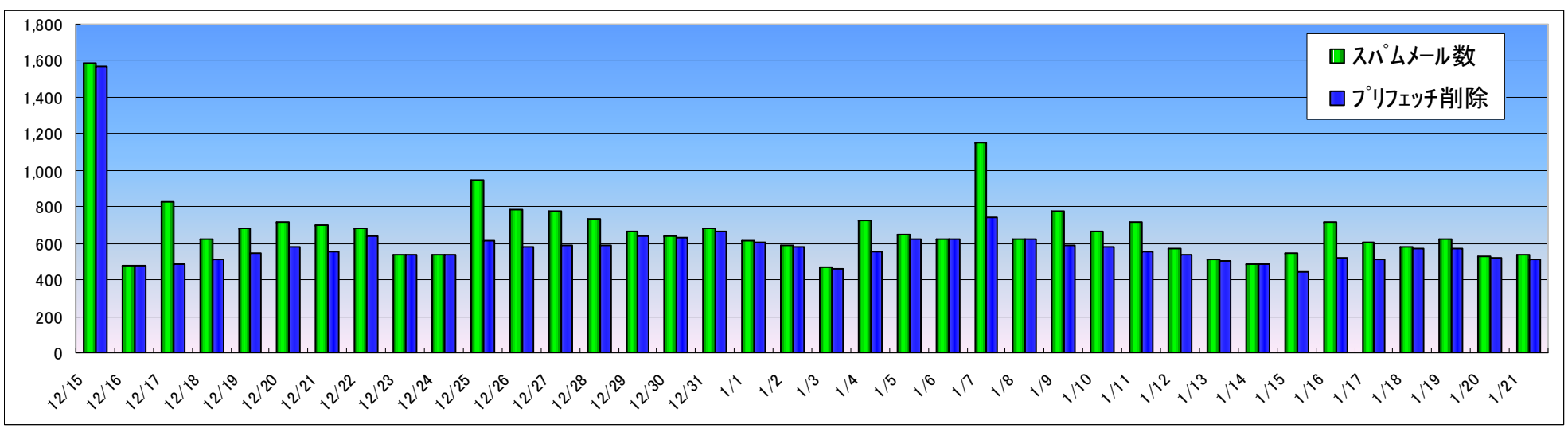
この評価より誤検知確率を少なくするスコアリングロジックでのクロスチェックが有効に働いていることがわかる。また、各検知手法が相互に補完し合っていることも推測できる。

お客様導入例

- ユーザ数　50ユーザ
- BLOCsystemによるスパムメール削除件数(月間)

	スパム数	秒数	時間	コスト/月	コスト/年
2007/12	9,945	29,835	8	41,438	497,250
2008/1	11,215	33,645	9	46,729	560,750

※削除時間を3秒、コスト時間単価5,000円で試算
毎日削除している作業時間をコスト試算すると、
年間約50万円以上の見えないコストが発生してたことが
わかります。



GIDEON BLOC system 管理画面

設置について

①お客様ネットワーク図
②メールサーバIPを確認(グローバルIP除外リストに指定)
③DNSサーバを確認(ホスティングの場合には、プロバイダDNSを設定)
④設置ネットワーク内にL3スイッチがある場合は、BLOCにルーティング
　設定が必要です。
⑤ルーターの設定変更　BLOCsystem IPアドレスの許可
⑥スパムメール転送先(メールボックス)を指定。
　　(誤検知によるメール紛失防止)
⑦判定速度
スパムと判定されたRBLやURLは高速化のためメモリにキャッシュされ、
その後も参照される。
また、スパムではないと判定されたメールの配信元IPアドレスやドメインも
「ノーマルキャッシュ」として同様に保存され、判定処理速度を向上させる
ために参照される。

サポートについて

・デモ機貸出サービスにより、事前に導入手順・動作確認が可能です。
（お貸出期間は2週間でお願いしております。）

・国内開発メーカーとして、お客様のご質問については24時間以内に
ご連絡をするサポートを心掛けております。

・BLOC system　GUI　サポート接続により、当社サポートセンターから
BLOC system内部設定を遠隔サポートが可能です。

筐体タイプ

- ご利用形態に応じて次の筐体タイプをお選びいただけます。

–小規模ユーザ(100ユーザ以内)

Lunch-Boxタイプ

[185×195×75mm（突起部を除く）]

–大中規模ユーザ(100ユーザ超) ※ユーザ数に応じてスペック(外寸)は異なります

タワーサーバタイプ

1Uタイプ

GIDEON

http://www.gideon.co.jp

製品に関するお問合せは弊社営業部

Tel: 045-590-1216

E-mail: sales@gideon.co.jp